

We claim:

- 1 1. A security gateway for securely connecting a plurality of networks; comprising:
2 a logical interface to a first network;
3 a logical interface to a second network;
4 a physical interface to a third network that is an untrusted network;
5 a logical interface to a fourth network that is a protected resource network;
6 a processor configured to execute packet handling rules for:
7 denying at least some client access through the gateway
8 from a host in the untrusted network to hosts in the first network,
9 in the second network and in the protected resource network;
10 denying at least some client access through the gateway
11 from a host in the second network to a host in the first network;
12 and
13 permitting at least some client access through the gateway
14 from a host in the first network to hosts in the second network and
15 in the protected resource network.
- 1 2. The security gateway of claim 1, wherein the processor is further configured to
2 execute packet handling rules for translating a source network address in a packet sent to
3 the second network.
- 1 3. The security gateway of claim 2, wherein the packet handling rules for translating
2 translate the source network address of a packet sent to the second network to be the
3 network address of the security gateway interface to the second network.
- 1 4. The security gateway of claim 1, wherein the processor is further configured to
2 execute packet handling rules for permitting at least some client access through the
3 gateway from a host in the first network to a host in the untrusted network.

1 5. The security gateway of claim 4, wherein the processor is further configured to
2 execute packet handling rules for translating a source network address in a packet sent to
3 the untrusted network.

1 6. The security gateway of claim 5, wherein the packet handling rules for translating
2 translate the source network address of a packet sent to the untrusted network to be the
3 network address of the security gateway interface to the untrusted network.

1 7. The security gateway of claim 1, wherein the processor is further configured to
2 execute packet handling rules for permitting at least some client access through the
3 gateway from a host in the protected resource network to a host in the first network.

1 8. The security gateway of claim 1, wherein the processor is further configured to
2 execute packet handling rules for denying at least some client access through the gateway
3 from a host in the protected resource network to a host in the first network.

1 9. The security gateway of claim 1, wherein the processor is further configured to
2 execute packet handling rules for permitting at least some client access through the
3 gateway from a host in the second network to a host in the untrusted network.

1 10. The security gateway of claim 9, wherein the processor is further configured to
2 execute packet handling rules for translating a source network address in a packet sent to
3 the untrusted network.

1 11. The security gateway of claim 10, wherein the packet handling rules for
2 translating translate the source network address of a packet sent to the untrusted network
3 to be the network address of the security gateway interface to the untrusted network.

1 12. The security gateway of claim 1, further comprising a protected network service,
2 and the processor is further configured to execute packet handling rules for denying at
3 least some access from at least one network to the protected network service.

1 13. The security gateway of claim 12, wherein the protected network service is a mail
2 relay.

1 14. The security gateway of claim 1, wherein the interface to the protected resource
2 network includes a VPN tunnel utilizing the untrusted network.

1 15. The security gateway of claim 1, wherein the processor is further configured to
2 execute packet handling rules for denying at least some client access through the gateway
3 from a host in the protected resource network to a host in the second network.

1 16. The security gateway of claim 1, wherein the processor is further configured to
2 execute packet handling rules for denying at least some client access through the gateway
3 from a host in the protected resource network to a host in the untrusted network.

1 17. The security gateway of claim 1, wherein the processor is further configured to
2 execute packet handling rules for denying at least some client access through the gateway
3 from a host in the second network to a host in the protected resource network.

1 18. The security gateway of claim 1, wherein the logical interface to the first network
2 is a logical interface to a first trust-group network, and the logical interface to the second
3 network is a logical interface to a second trust-group network.

1 19. The security gateway of claim 1, wherein the logical interface to the first network
2 is a logical interface to a first local network, and the logical interface to the second
3 network is a logical interface to a second local network.

1 20. The security gateway of claim 1, wherein the logical interface to the protected
2 resource network is a logical interface to a remote corporate network.

1 21. The security gateway of claim 1, wherein the processor is further configured to
2 execute packet handling rules for:
3 denying at least some client access through the gateway from a
4 host in the second network to a host in the protected resource network; and
5 denying at least some client access through the gateway from a
6 host in the protected resource network to hosts in the second network and
7 in the untrusted network.

1 22. The security gateway of claim 21, wherein the interface to the protected resource
2 network includes a VPN tunnel utilizing the untrusted network.

1 23. The security gateway of claim 22, wherein the processor is further configured to
2 execute packet handling rules for permitting at least some client access through the
3 gateway from a host in the second network to a host in the untrusted network.

1 24. The security gateway of claim 23, wherein the processor is further configured to
2 execute packet handling rules for permitting at least some client access through the
3 gateway from a host in the first network to a host in the untrusted network.

1 25. A machine readable medium containing configuration instructions for performing
2 a method for securely connecting a plurality of networks through a security gateway
3 having a logical interface to a first network, a logical interface to a second network, a
4 physical interface to a third network that is an untrusted network and a logical interface to
5 a fourth network that is a protected resource network, the method comprising the steps of:
6 denying at least some client access through the gateway from a host in the
7 untrusted network to hosts in the first network, in the second network and in the protected
8 resource network;
9 denying at least some client access through the gateway from a host in the
10 second network to a host in the first network; and
11 permitting at least some client access through the gateway from a host in
12 the first network to hosts in the second network and in the protected resource network.

1 26. The machine readable medium of claim 25, wherein the method further comprises
2 the step of translating a source network address in a packet sent to the second local
3 network.

1 27. The machine readable medium of claim 26, wherein the translating step includes
2 translating the source network address of a packet sent to the second network to be the
3 network address of the security gateway interface to the second network.

1 28. The machine readable medium of claim 25, wherein the method further comprises
2 the step of permitting at least some client access through the gateway from a host in the
3 first network to a host in the untrusted network.

1 29. The machine readable medium of claim 28, wherein the method further comprises
2 the step of translating a source network address in a packet sent to the untrusted network.

1 30. The machine readable medium of claim 29, wherein the translating step includes
2 translating the source network address of a packets sent to the untrusted network to be the
3 network address of the security gateway interface to the untrusted network.

1 31. The machine readable medium of claim 25, wherein the method further comprises
2 the step of permitting at least some client access through the gateway from a host in the
3 protected resource network to a host in the first network.

1 32. The machine readable medium of claim 25, wherein the method further comprises
2 the step of denying at least some client access through the gateway from a host in the
3 protected resource network to a host in the first network.

1 33. The machine readable medium of claim 25, wherein the method further comprises
2 the step of permitting at least some client access through the gateway from a host in the
3 second network to a host in the untrusted network.

1 34. The machine readable medium of claim 33, wherein the method further comprises
2 the step of translating a source network address in a packet sent to the untrusted network.

1 35. The machine readable medium of claim 34, wherein the translating step includes
2 translating the source network address of a packet sent to the untrusted network to be the
3 network address of the security gateway interface to the untrusted network.

1 36. The machine readable medium of claim 25, wherein the security gateway further
2 has a protected network service, and the method further comprises the step of denying at
3 least some access from at least one network to the protected network service.

1 37. The machine readable medium of claim 36, wherein the protected network service
2 is a mail relay.

1 38. The machine readable medium of claim 25, wherein the interface to the protected
2 resource network includes a VPN tunnel utilizing the untrusted network.

1 39. The machine readable medium of claim 25, wherein the method further comprises
2 the step of denying at least some client access through the gateway from a host in the
3 protected resource network to a host in the second network.

1 40. The machine readable medium of claim 25, wherein the method further comprises
2 the step of denying at least some client access through the gateway from a host in the
3 protected resource network to a host in the untrusted network.

1 41. The machine readable medium of claim 25, wherein the method further comprises
2 the step of denying at least some client access through the gateway from a host in the
3 second network to a host in the protected resource network.

1 42. A method for securely connecting a plurality of networks through a security
2 gateway having a logical interface to a first network, a logical interface to a second
3 network, a physical interface to a third network that is an untrusted network and a logical
4 interface to a fourth network that is a protected resource network; the method comprising
5 the steps of:

6 denying at least some client access through the gateway from a host in the
7 untrusted network to hosts in the first network, in the second network and in the protected
8 resource network;

9 denying client access from a host in the second network to a host in the
10 first network; and

11 permitting client access from a host in the first network to hosts in the
12 second network and in the protected resource network.

1 43. The method of claim 42, further comprising the step of translating a source
2 network address in a packet sent to the second network.

1 44. The method of claim 43, wherein the translating step includes translating the
2 source network address of a packet sent to the second network to be the network address
3 of the security gateway interface to the second network.

1 45. The method of claim 42, further comprising the step of permitting at least some
2 client access through the gateway from a host in the first network to a host in the
3 untrusted network.

1 46. The method of claim 45, further comprising the step of translating a source
2 network address in a packet sent to the untrusted network.

1 47. The method of claim 46, wherein the translating step includes translating the
2 source network address of a packet sent to the untrusted network to be the network
3 address of the security gateway interface to the untrusted network.

1 48. The method of claim 42, further comprising the step of permitting at least some
2 client access through the gateway from a host in the protected resource network to a host
3 in the first network.

1 49. The method of claim 42, further comprising the step of denying at least some
2 client access through the gateway from a host in the protected resource network to a host
3 in the first network.

1 50. The method of claim 42, further comprising the step of permitting at least some
2 client access through the gateway from a host in the second network to a host in the
3 untrusted network.

1 51. The method of claim 50, further comprising the step of translating a source
2 network address in a packet sent to the untrusted network.

1 52. The method of claim 51, wherein the translating step includes translating the
2 source network address of a packet sent to the untrusted network to be the network
3 address of the security gateway interface to the untrusted network.

1 53. The method of claim 52, wherein the security gateway further has a protected
2 network service, and the method further comprises the step of denying at least some
3 access from at least one network to the protected network service.

1 54. The method of claim 53, wherein the protected network service is a mail relay.

1 55. The method of claim 42, wherein the interface to the protected resource network
2 includes a VPN tunnel utilizing the untrusted network.

1 56. The method of claim 42, further comprising the step of denying at least some
2 client access through the gateway from a host in the protected resource network to a host
3 in the second network.

1 57. The method of claim 42, further comprising the step of denying at least some
2 client access through the gateway from a host in the protected resource network to a host
3 in the untrusted network.

1 58. The method of claim 42, further comprising the step of denying at least some
2 client access through the gateway from a host in the second network to a host in the
3 protected resource network.